Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERT-FR

Paris, le 19 avril 2017
N° CERTFR-2017-AVI-122

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans Oracle MySQL

Gestion du document

Référence	CERTFR-2017-AVI-122
Titre	Multiples vulnérabilités dans Oracle MySQL
Date de la première version	19 avril 2017
Date de la dernière version	–
Source(s)	Bulletin de sécurité Oracle cpuapr2017-3236618 du 18 avril 2017 Bulletin de sécurité Oracle cpuapr2017verbose-3236619 du 18 avril 2017
Pièce(s) jointe(s)	Aucune

TAB. 1 – *Gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

1 - Risque(s)

- exécution de code arbitraire à distance
- déni de service à distance
- atteinte à l'intégrité des données
- atteinte à la confidentialité des données

2 - Systèmes affectés

- Oracle MySQL Enterprise Monitor versions 3.1.6.8003 et antérieures
- Oracle MySQL Enterprise Monitor versions 3.2.1182 et antérieures
- Oracle MySQL Enterprise Monitor versions 3.3.2.1162 et antérieures
- Oracle MySQL Workbench versions 6.3.8 et antérieures
- Oracle MySQL Enterprise Backup versions 3.12.3 et antérieures
- Oracle MySQL Enterprise Backup versions 4.0.3 et antérieures
- Oracle MySQL Server versions 5.5.54 et antérieures
- Oracle MySQL Server versions 5.6.35 et antérieures
- Oracle MySQL Server versions 5.7.17 et antérieures
- Oracle MySQL Connectors versions 5.1.41 et antérieures
- Oracle MySQL Cluster versions 7.2.27 et antérieures

- Oracle MySQL Cluster versions 7.3.16 et antérieures
- Oracle MySQL Cluster versions 7.4.14 et antérieures
- Oracle MySQL Cluster versions 7.5.5 et antérieures
- Oracle MySQL Connectors versions 2.1.5 et antérieures

3 - Résumé

De multiples vulnérabilités ont été corrigées dans *Oracle MySQL*. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, un déni de service à distance et une atteinte à l'intégrité des données.

4 - Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

5 - Documentation

- Bulletin de sécurité Oracle cpuapr2017-3236618 du 18 avril 2017
  http://www.oracle.com/technetwork/security-advisory/cpuapr2017-3236618.html
- Bulletin de sécurité Oracle cpuapr2017verbose-3236619 du 18 avril 2017
  http://www.oracle.com/technetwork/security-advisory/cpuapr2017verbose-3236619.html#MSQL
- Référence CVE CVE-2016-2176
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2176
- Référence CVE CVE-2016-3092
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3092
- Référence CVE CVE-2016-6303
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6303
- Référence CVE CVE-2017-3302
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3302
- Référence CVE CVE-2017-3304
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3304
- Référence CVE CVE-2017-3305
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3305
- Référence CVE CVE-2017-3306
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3306
- Référence CVE CVE-2017-3307
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3307
- Référence CVE CVE-2017-3308
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3308
- Référence CVE CVE-2017-3309
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3309
- Référence CVE CVE-2017-3329
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3329
- Référence CVE CVE-2017-3331
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3331
- Référence CVE CVE-2017-3450
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3450
- Référence CVE CVE-2017-3452
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3452
- Référence CVE CVE-2017-3453
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3453
- Référence CVE CVE-2017-3454
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3454

- Référence CVE CVE-2017-3455
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3455
- Référence CVE CVE-2017-3456
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3456
- Référence CVE CVE-2017-3457
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3457
- Référence CVE CVE-2017-3458
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3458
- Référence CVE CVE-2017-3459
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3459
- Référence CVE CVE-2017-3460
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3460
- Référence CVE CVE-2017-3461
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3461
- Référence CVE CVE-2017-3462
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3462
- Référence CVE CVE-2017-3463
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3463
- Référence CVE CVE-2017-3464
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3464
- Référence CVE CVE-2017-3465
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3465
- Référence CVE CVE-2017-3467
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3467
- Référence CVE CVE-2017-3468
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3468
- Référence CVE CVE-2017-3469
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3469
- Référence CVE CVE-2017-3586
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3586
- Référence CVE CVE-2017-3589
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3589
- Référence CVE CVE-2017-3590
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3590
- Référence CVE CVE-2017-3599
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3599
- Référence CVE CVE-2017-3600
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3600
- Référence CVE CVE-2017-3731
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3731
- Référence CVE CVE-2017-3732
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3732
- Référence CVE CVE-2017-5638
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5638

Gestion détaillée du document

19 avril 2017 version initiale.